

POLYNOMIAL FUNCTIONS IN THE RESIDUE CLASS RINGS OF POLYNOMIALS OVER FINITE FIELDS

XIUMEI LI AND MIN SHA

ABSTRACT. In this paper, as an analogue of the integer case, we define polynomial functions over the residue class rings of polynomials over a finite field, and then we give canonical representations and the counting formula for such polynomial functions.

1. INTRODUCTION

1.1. Motivation. Let m and n be two positive integers. In [5] Chen has defined the concept of a polynomial function from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ and has obtained an exact formula for the number of such polynomial functions, which has been extended by Chen [6] to functions from $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. For the case when $n = m$, there are many related earlier results which could refer to [4, 7, 8, 10, 11]. Especially, Bhargava [2, 3] has considerably enlarge the setting for polynomial functions by replacing “the rational integers \mathbb{Z} ” with “Dedekind domain”.

In this paper, we want to generalize the above concept of polynomial function to the case of residue class rings of polynomials over a finite field, as well as consider its canonical representation and counting formula by following the same strategy as in [5, 6].

1.2. Our situation. Let \mathbb{F}_q be the finite field of q elements, where q is a power of a prime p . Denote by $R = \mathbb{F}_q[t]$ the polynomial ring of one variable over \mathbb{F}_q . For any non-constant polynomial $n \in R$, let R_n be the residue class ring of R modulo n , and let

$$\mathcal{R}_n = \{i \in R : \deg i < \deg n\}.$$

Note that \mathcal{R}_n is a complete set of the representatives of residue classes modulo n . So, if $\deg n = \deg m$, then R_n and R_m have the same complete set of representatives of residue classes.

2010 *Mathematics Subject Classification.* 11T06, 11T55.

Key words and phrases. Polynomial function, factorial, polynomial over a finite field, residue class ring.

From now on, let n_1, \dots, n_r, m be non-constant polynomials in R ($r \geq 1$).

Definition 1.1. A function $f : R_{n_1} \times \dots \times R_{n_r} \rightarrow R_m$ is said to be a *polynomial function*, if it is representable by a polynomial $F \in R[x_1, \dots, x_r]$ such that

$$f(b_1, \dots, b_r) \equiv F(b_1, \dots, b_r) \pmod{m}$$

for any $(b_1, \dots, b_r) \in \mathcal{R}_{n_1} \times \dots \times \mathcal{R}_{n_r}$, where (b_1, \dots, b_r) is considered as an element in R^r when evaluating $F(b_1, \dots, b_r)$.

In this paper, the main aim is to count the polynomial functions from $R_{n_1} \times \dots \times R_{n_r}$ to R_m by giving their canonical representations.

Let \mathbb{N} be the set of non-negative integers. We write $\mathbb{F}_q = \{a_0 = 0, a_1, \dots, a_{q-1}\}$ throughout the paper, and for every $k \in \mathbb{N}$, let

$$a_k = a_{c_0} + a_{c_1}t + \dots + a_{c_h}t^h,$$

where $\sum_{i=0}^h c_i q^i$ is the q -adic expansion of k . This gives us a one-to-one correspondence between \mathbb{N} and $\mathbb{F}_q[t]$.

Now, we can define a factorial function for polynomials in R , which is an analogue of factorials of non-negative integers; see [9, 12] for other analogues.

Definition 1.2. For every $k \in \mathbb{N}$, we define the factorial of k denoted by $k!$ as follows. If $k = 0$, $k! = 1$; otherwise,

$$k! = \prod_{i=0}^{k-1} (a_k - a_i),$$

which can be viewed as the factorial of a_k . For a vector $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$, we define

$$\mathbf{k}! = \prod_{i=1}^r k_i!.$$

Throughout the paper, for any non-negative integer k , the meaning of “ $k!$ ” is exactly the one in Definition 1.2. The reader should not confuse this with the classical case.

Let $R[x_1, \dots, x_r]$ be the polynomial ring of r variables over R . Using factorials, we can define a basis for $R[x_1, \dots, x_r]$ over R . We first define an ordering in \mathbb{N}^r .

Definition 1.3. For any $\mathbf{k} = (k_1, \dots, k_r)$ and $\mathbf{h} = (h_1, \dots, h_r)$, we say that \mathbf{k} is less than \mathbf{h} , denoted by $\mathbf{k} < \mathbf{h}$, if there exists j such that $k_j < h_j$ and $k_i = h_i$ for all $i < j$. As usual, $\mathbf{k} \leq \mathbf{h}$ means that $\mathbf{k} < \mathbf{h}$ or $\mathbf{k} = \mathbf{h}$.

Definition 1.4. For any $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$, we define

$$(\mathbf{x})_{\mathbf{k}} = \prod_{i=1}^r (x_i)_{k_i},$$

where $(x_i)_{k_i}$ is defined as follows:

$$(x_i)_{k_i} = 1 \text{ if } k_i = 0, \text{ otherwise } (x_i)_{k_i} = \prod_{j=0}^{k_i-1} (x_i - a_j).$$

Clearly, the polynomials $(\mathbf{x})_{\mathbf{k}}, \mathbf{k} \in \mathbb{N}^r$, form an R -basis for $R[x_1, \dots, x_r]$.

1.3. Notation and convention. From now on, we fix non-constant polynomials $m, n_1, \dots, n_r \in R$. Define

- $\lambda(m)$ = the smallest positive integer λ such that $m \mid \lambda!$,
- $\mu(m, n_i) = \min\{\lambda(m), q^{\deg n_i}\}$ for $i = 1, \dots, r$.

Without confusion we write λ and μ_i instead of $\lambda(m)$ and $\mu(m, n_i)$ for simplicity, and define a vector of non-negative integers

$$\boldsymbol{\mu} = (\mu_1 - 1, \dots, \mu_r - 1).$$

The symbol \equiv will always denote the congruence $(\text{mod } m)$. The capital letters F, G, \dots represents the elements in $R[x_1, \dots, x_r]$. We define a relation \sim in $R[x_1, \dots, x_r]$ as follows: $F \sim G$ if and only if F and G represent the same polynomial function from $R_{n_1} \times \dots \times R_{n_r}$ to R_m .

2. MAIN RESULTS

We first determine under which condition every function from $R_{n_1} \times \dots \times R_{n_r}$ to R_m is a polynomial function.

Theorem 2.1. *Every function $f : R_{n_1} \times \dots \times R_{n_r} \rightarrow R_m$ is a polynomial function if and only if for any $i = 1, \dots, r$, the degree of n_i is not greater than the degree of any non-constant factor of m .*

Proof. We first prove the necessary part by contradiction. Without loss of generality, suppose that there is a non-constant factor of m , say b , such that $\deg n_1 > \deg b$. So, $(0, 0, \dots, 0)$ and $(b, 0, \dots, 0)$ are two distinct elements in $R_{n_1} \times \dots \times R_{n_r}$. Then, for any function $f : R_{n_1} \times \dots \times R_{n_r} \rightarrow R_m$, if it is represented by a polynomial $F \in R[x_1, \dots, x_r]$, we have

$$F(0, 0, \dots, 0) \equiv F(b, 0, \dots, 0) \pmod{b}.$$

This means that the choices of $f(0, 0, \dots, 0)$ and $f(b, 0, \dots, 0)$ are not independent. This contradicts with the assumption.

Now, we prove the sufficient part. Since for each i , $\deg n_i$ is not greater than the degree of any non-constant factor of m , we have $\gcd(j-l, m) = 1$ for any $j, l \in \mathcal{R}_{n_i}$ with $j \neq l$. Then, $j-l$ gives a unit in R_m , and we use $b_{j,l}^i$ to denote the inverse of $j-l$ in R_m .

Let $f : R_{n_1} \times \cdots \times R_{n_r} \rightarrow R_m$ be a function. By the Lagrange interpolation, for any $(j_1, \dots, j_r) \in \mathcal{R}_{n_1} \times \cdots \times \mathcal{R}_{n_r}$ we have

$$f(j_1, \dots, j_r) = \sum_{(l_1, \dots, l_r) \in \mathcal{R}_{n_1} \times \cdots \times \mathcal{R}_{n_r}} f(l_1, \dots, l_r) \prod_{i=1}^r \prod_{s \in \mathcal{R}_{n_i}, s \neq l_i} b_{l_i, s}^i (j_i - s).$$

Thus, f is a polynomial function represented by the polynomial

$$F(x_1, \dots, x_r) = \sum_{(l_1, \dots, l_r) \in \mathcal{R}_{n_1} \times \cdots \times \mathcal{R}_{n_r}} f(l_1, \dots, l_r) \prod_{i=1}^r \prod_{s \in \mathcal{R}_{n_i}, s \neq l_i} b_{l_i, s}^i (x_i - s).$$

This completes the proof. \square

We now state a canonical representation of a polynomial function from $R_{n_1} \times \cdots \times R_{n_r}$ to R_m .

Theorem 2.2. *Let f be a polynomial function from $R_{n_1} \times \cdots \times R_{n_r}$ to R_m . Then, f can be uniquely represented by a polynomial*

$$F = \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}},$$

where the coefficients $b_{\mathbf{k}} \in R$ satisfy

$$b_{\mathbf{k}} \in R, \quad b_{\mathbf{k}} = 0 \quad \text{or} \quad \deg b_{\mathbf{k}} < \deg \frac{m}{\gcd(m, \mathbf{k}!)}.$$

From Theorem 2.2, we immediately obtain the following counting formula.

Theorem 2.3. *The number of polynomial functions from $R_{n_1} \times \cdots \times R_{n_r}$ to R_m is given by*

$$N(n_1, \dots, n_r, m) = \prod_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} q^{\deg \frac{m}{\gcd(m, \mathbf{k}!)}}.$$

We remark that if $r = 1$ and $n_1 = m$, then there is another form of the counting formula implied in [2, Corollary 2].

In order to prove Theorem 2.2, we need to make some preparations.

Lemma 2.4. *Let $F \in R[x_1, \dots, x_r]$, and let \mathbf{j} be a vector of non-negative integers. Then*

$$F = Q_{\mathbf{j}}(\mathbf{x})_{\mathbf{j}} + \sum_{0 \leq \mathbf{k} < \mathbf{j}} c_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}},$$

where $Q_{\mathbf{j}} \in R[x_1, \dots, x_r]$ and $c_{\mathbf{k}} \in R$ are uniquely determined by F .

Proof. The result follows from the fact that $\{(\mathbf{x})_{\mathbf{k}} : \mathbf{k} \in \mathbb{N}^r\}$ is an R -basis of $R[x_1, \dots, x_r]$. \square

Lemma 2.5. *For any $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$ and any $\mathbf{x} = (x_1, \dots, x_r) \in R^r$, we have*

$$\mathbf{k}! \mid (\mathbf{x})_{\mathbf{k}}.$$

Proof. It has been indicated in [3, Section 10] (see also the example in page 289 of [1]) that for any $s \in \mathbb{N}$ and any $g \in R$, we have

$$s! \mid (g)_s = \prod_{i=0}^{s-1} (g - a_i).$$

So, for each i , $k_i! \mid (x_i)_{k_i}$. This implies the desired result. \square

Lemma 2.6. *Let $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$, and assume that $k_i \geq \mu_i$ for some i . Then, $(\mathbf{x})_{\mathbf{k}} \sim 0$.*

Proof. By definition, it suffices to prove that $(x_i)_{k_i} \sim 0$.

If $\lambda \leq q^{\deg n_i}$, then $\mu_i = \lambda$, and so $k_i \geq \lambda$. Thus, we have $\lambda! \mid k_i!$. Then from Lemma 2.5 and the definition of λ , $m \mid (g)_{k_i}$ for any $g \in R$. This implies that $(x_i)_{k_i} \sim 0$.

If $\lambda > q^{\deg n_i}$, then $\mu_i = q^{\deg n_i}$ so that $k_i \geq q^{\deg n_i}$. By definition, we have $(g)_{k_i} = 0$ for any $g \in \mathcal{R}_{n_i}$, which implies that $(x_i)_{k_i} \sim 0$. \square

Lemma 2.7. $\sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$ if and only if $b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$ for all $0 \leq \mathbf{k} \leq \boldsymbol{\mu}$.

Proof. Clearly, we only need to show the necessity.

The necessity is trivial when $\boldsymbol{\mu} = 0$. Now, we assume that $\boldsymbol{\mu} > 0$. Suppose that

$$\sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0.$$

Then, we have

$$\sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(0)_{\mathbf{k}} \equiv 0,$$

which, together with $(0)_{\mathbf{k}} = 0$ for any $\mathbf{k} > 0$, yields that $b_0 \equiv 0$. So, $b_0(\mathbf{x})_0 \sim 0$.

Now we proceed by induction. Assume that there is $\mathbf{h} = (h_1, \dots, h_r) \leq \boldsymbol{\mu}$ such that $b_{\mathbf{j}}(\mathbf{x})_{\mathbf{j}} \sim 0$ for all $\mathbf{j} < \mathbf{h}$. We shall show that $b_{\mathbf{h}}(\mathbf{x})_{\mathbf{h}} \sim 0$. From the induction hypothesis and the original condition that

$$\sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0,$$

we have

$$\sum_{h \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0.$$

By definition, if $\mathbf{a} = (a_{h_1}, \dots, a_{h_r})$, we get $(\mathbf{a})_j = 0$ for any $j > \mathbf{h}$ and $(\mathbf{a})_{\mathbf{h}} = \prod_{i=1}^r h_i!$. Thus, we obtain $b_{\mathbf{h}} \prod_{i=1}^r h_i! \equiv 0$. Then, by Lemma 2.5, we have $b_{\mathbf{h}}(\mathbf{x})_{\mathbf{h}} \sim 0$. This in fact completes the proof. \square

Lemma 2.8. *Let $\mathbf{k} = (k_1, \dots, k_r)$ with $0 \leq k_i \leq q^{\deg n_i} - 1$ for $i = 1, \dots, r$. Then, $b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$ if and only if*

$$\frac{m}{\gcd(m, \mathbf{k}!)} \mid b_{\mathbf{k}}.$$

Proof. First, suppose that $b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$, and let $\mathbf{a} = (a_{k_1}, \dots, a_{k_r})$. Then, since $0 \leq k_i \leq q^{\deg n_i} - 1$ (that is, $a_{k_i} \in \mathcal{R}_{n_i}$) for each i , we have $b_{\mathbf{k}}(\mathbf{a})_{\mathbf{k}} \equiv 0$. Noticing $(\mathbf{a})_{\mathbf{k}} = \mathbf{k}!$, we get $b_{\mathbf{k}} \mathbf{k}! \equiv 0$, and so $m \mid b_{\mathbf{k}} \mathbf{k}!$. Thus, we have

$$\frac{m}{\gcd(m, \mathbf{k}!)} \mid b_{\mathbf{k}}.$$

Conversely, if

$$\frac{m}{\gcd(m, \mathbf{k}!)} \mid b_{\mathbf{k}},$$

we have $m \mid b_{\mathbf{k}} \mathbf{k}!$. Then, it follows from Lemma 2.5 that $b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$. \square

Now, we are ready to prove Theorem 2.2.

Proof of Theorem 2.2. Let G be an arbitrary polynomial representation of f , and let $\boldsymbol{\mu}^+$ be the smallest vector in \mathbb{N}^r greater than $\boldsymbol{\mu}$. In fact, $\boldsymbol{\mu}^+ = (\mu_1 - 1, \dots, \mu_{r-1} - 1, \mu_r)$. By Lemma 2.4, we write

$$G = Q_{\boldsymbol{\mu}^+}(\mathbf{x})_{\boldsymbol{\mu}^+} + \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} c_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}},$$

where $Q_{\boldsymbol{\mu}^+} \in R[x_1, \dots, x_r]$ and $c_{\mathbf{k}} \in R$ are uniquely determined by G . By the division algorithm for polynomials, we have

$$c_{\mathbf{k}} = q_{\mathbf{k}} \cdot \frac{m}{\gcd(m, \mathbf{k}!)} + b_{\mathbf{k}}$$

with $b_{\mathbf{k}} = 0$ or $\deg b_{\mathbf{k}} < \deg \frac{m}{\gcd(m, \mathbf{k}!)}$, where $q_{\mathbf{k}}, b_{\mathbf{k}} \in R$ are uniquely determined by $c_{\mathbf{k}}$. Then

$$\begin{aligned} G &= Q_{\boldsymbol{\mu}^+}(\mathbf{x})_{\boldsymbol{\mu}^+} + \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} (q_{\mathbf{k}} \cdot \frac{m}{\gcd(m, \mathbf{k}!)} + b_{\mathbf{k}})(\mathbf{x})_{\mathbf{k}} \\ &= Q_{\boldsymbol{\mu}^+}(\mathbf{x})_{\boldsymbol{\mu}^+} + \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} q_{\mathbf{k}} \cdot \frac{m}{\gcd(m, \mathbf{k}!)}(\mathbf{x})_{\mathbf{k}} + \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}}. \end{aligned}$$

So, $G - \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}} \sim 0$ by Lemmas 2.6 and 2.8. Therefore,

$$G \sim \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}},$$

which means that f is representable by the polynomial

$$F = \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}}(\mathbf{x})_{\mathbf{k}}$$

with $b_{\mathbf{k}} = 0$ or $\deg b_{\mathbf{k}} < \deg \frac{m}{\gcd(m, \mathbf{k}!)}$.

The uniqueness of such a representation follows directly from Lemmas 2.7 and 2.8. \square

Applying Theorem 2.3, we can get a simpler canonical representation for a polynomial function from $R_{n_1} \times \cdots \times R_{n_r}$ to R_m .

Theorem 2.9. *Let f be a polynomial function from $R_{n_1} \times \cdots \times R_{n_r}$ to R_m . Then, f can be uniquely represented by a polynomial*

$$F = \sum_{0 \leq \mathbf{k} \leq \boldsymbol{\mu}} b_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}, \quad b_{\mathbf{k}} \in R, \quad b_{\mathbf{k}} = 0 \quad \text{or} \quad \deg b_{\mathbf{k}} < \deg \frac{m}{\gcd(m, \mathbf{k}!)},$$

where $\mathbf{x}^{\mathbf{k}}$ with $\mathbf{x} = (x_1, \dots, x_r)$ and $\mathbf{k} = (k_1, \dots, k_r)$ means $x_1^{k_1} \cdots x_r^{k_r}$.

In order to prove Theorem 2.9, we need the following lemma. Each monomial $x_1^{k_1} \cdots x_r^{k_r} \in R[x_1, \dots, x_r]$ corresponds to an integer vector $(k_1, \dots, k_r) \in \mathbb{N}^r$. For any $F \in R[x_1, \dots, x_r]$, let $lt(F)$ be the maximal integer vector coming from the monomials in F .

Lemma 2.10. *Let $F \in R[x_1, \dots, x_r]$ be a polynomial with $lt(F) \leq \boldsymbol{\mu}$. Then, there are $b_{\mathbf{k}} \in R, 0 \leq \mathbf{k} \leq lt(F)$ with $b_{\mathbf{k}} = 0$ or $\deg b_{\mathbf{k}} < \deg \frac{m}{\gcd(m, \mathbf{k}!)}$ such that*

$$F \sim \sum_{0 \leq \mathbf{k} \leq lt(F)} b_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}.$$

Proof. We prove the desired result by induction on $lt(F)$. It is trivial for $lt(F) = 0$. Let $lt(F) > 0$ and write

$$F = \sum_{0 \leq \mathbf{k} \leq lt(F)} d_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}, \quad d_{\mathbf{k}} \in R.$$

Denote $\mathbf{j} = lt(F)$. By the division algorithm, we obtain

$$d_{\mathbf{j}} = q_{\mathbf{j}} \cdot \frac{m}{\gcd(m, \mathbf{j}!)} + b_{\mathbf{j}},$$

where $b_{\mathbf{j}} = 0$ or $\deg b_{\mathbf{j}} < \deg \frac{m}{\gcd(m, \mathbf{j}!)}$. Put

$$G = F - q_{\mathbf{j}} \cdot \frac{m}{\gcd(m, \mathbf{j}!)} \cdot (\mathbf{x})_{\mathbf{j}}.$$

Then, by Lemma 2.8 we have $F \sim G$. Noticing that

$$G = b_{\mathbf{j}}x^{\mathbf{j}} + H$$

for some polynomial $H \in R[x_1, \dots, x_r]$ with $lt(H) < \mathbf{j} = lt(F)$ and applying the induction hypothesis to H , we conclude the proof. \square

Now, we can prove Theorem 2.9.

Proof of Theorem 2.9. The existence of such a representation F follows directly from Theorem 2.2 and Lemma 2.10. The uniqueness of the representation is clear from the fact that the number of the representations here is the same as those in Theorem 2.2. \square

ACKNOWLEDGEMENT

The research of Xiumei Li was supported by National Science Foundation of China Grant No. 11526119 and Scientific Research Foundation of Qufu Normal University No. BSQD20130139. The research of M. S. was supported by the Macquarie University Research Fellowship.

REFERENCES

- [1] D. Adam, *Simultaneous orderings in function fields*, J. Number Theory **112** (2005), 287–297.
- [2] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. reine angew. Math. **490** (1997), 101–127.
- [3] M. Bhargava, *The factorial function and generalizations*, Amer. Math. Monthly **107** (2000), 783–799.
- [4] L. Carlitz, *Functions and polynomials (mod p^n)*, Acta Arith. **9** (1964), 67–78.
- [5] Z. Chen, *On polynomial functions from \mathbb{Z}_n to \mathbb{Z}_m* , Discrete Math. **137** (1995), 137–145.
- [6] Z. Chen, *On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}$ to \mathbb{Z}_m* , Discrete Math. **162** (1996), 67–76.
- [7] G. Keller and F. R. Olson, *Counting polynomial functions (mod p^n)*, Duke Math. J. **35** (1968), 835–838.
- [8] A. J. Kempner, *Polynomials and their residue systems*, Trans. Amer. Math. Soc. **22** (1921), 240–288.
- [9] X. Li and M. Sha, *Gauss factorials of polynomials over finite fields*, Int. J. Number Theory, to appear, DOI: <http://dx.doi.org/10.1142/S1793042117501093>.
- [10] G. Mullen and H. Stevens, *Polynomial functions (mod m)*, Acta. Math. Ac. Sci. Hung. **44** (1984), 237–241.
- [11] D. Singmaster, *On Polynomial functions (mod m)*, J. Number Theory **6** (1974), 345–352.
- [12] D. S. Thakur, *Binomial and factorial congruences for $\mathbb{F}_q[t]$* , Finite Fields Th. App. **18** (2012), 271–282.

SCHOOL OF MATHEMATICAL SCIENCES, QUFU NORMAL UNIVERSITY, QUFU,
SHANDONG, 273165, CHINA

E-mail address: `lxiumei2013@hotmail.com`

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, SYDNEY, NSW 2109,
AUSTRALIA

E-mail address: `shamin2010@gmail.com`